To:

T-Mobile USA, Inc.
Customer Relations & Legal Department
12920 SE 38th St, Bellevue, WA 98006
Email: executive.relations@t-mobile.com

legalnotice@t-mobile.com

privacy@t-mobile.com

Date: May 24, 2025

Via Certified Mail & Email

From:
John R. Fouts
502-956-0052 (text only – ADA)

502-996-8246 (fax-HIPAA Compliant)
icreateupwardspirals@gmail.com
[Formerly: fouts.john@gmail.com]

Subject: Urgent Formal Complaint and Demand for Escalation — Device Interference, Unlawful Interception, and Failure to Investigate

Date: 2025-05-24

I. Overview of Issues

I am submitting this letter as a formal legal notice and demand for immediate resolution and investigative escalation regarding multiple severe failures by T-Mobile involving:

- **Confirmed unlawful digital surveillance and signal interception**
- **Network compromise tied to spoofed towers and redirected traffic**
- **Systemic failures in internal fraud and network security escalation pathways**
- **Failure to acknowledge or follow up on multiple documented reports**

These failures have directly endangered the safety and legal rights of myself and my disabled child, and they constitute a potential breach of federal telecommunications law, including but not limited to the **Wiretap Act (18 U.S. Code § 2511)**, the **Communications Act of 1934**, and civil rights protections under the **ADA and Section 504**.

II. Specific Incidents and Failures

1. **TOWER SPOOFING / SIGNAL REDIRECTION**
   My phone has been repeatedly observed connecting to non-public, unidentified towers not listed in FCC databases, resulting in call rerouting, dropped communications, and possible packet inspection.

2. **UNRESOLVED DEVICE COMPROMISE**
   Device diagnostics, including analytics reports and security alerts from Apple, confirm network-based anomalies. Your support representatives escalated to "fraud" and "network engineering," yet no legitimate investigation or remedy was provided.

3. **FAILURE TO FOLLOW THROUGH**
   I was promised follow-up from your fraud and engineering teams. Instead, I only received generic customer satisfaction surveys and no substantive communication. This lack of action constitutes negligence.

4. **OBSTRUCTION OF LEGAL ACCESS**
   I am currently engaged in federal civil rights litigation and FOIA filings. T-Mobile's failure to respond or investigate prevents me from communicating securely and accessing legal recourse.

III. Demands for Resolution

I demand that T-Mobile immediately:

- Escalate this issue to **your internal legal and security teams**
- Provide a IT-forensic-level-audit **complete network log of device connection records** for the affected period (Jun 2022–present), including tower IDs and IP pathing
- Disclose whether **third parties or law enforcement** have ever accessed my data without a subpoena or notification
- I explicitly and unequivocally do not consent to any form of surveillance, tracking, data harvesting, or unauthorized monitoring of my communications, devices, location, or digital activity.
- **I further require full disclosure from T-Mobile regarding any unauthorized, unregistered, rogue, or spoofed tower infrastructure that my device(s) have been connected to—whether through direct handoff, forced redirection, or temporary authentication attempts.** This includes any anomalies or logs involving IMSI catchers, rogue cell simulators, or unexplained handovers to non-T-Mobile-owned towers. Additionally, you are required to provide a technical explanation for the ongoing low or erratic signal strength, tower misassociation, and routing inconsistencies I have experienced across multiple devices and locations—especially where

public coverage maps show strong expected service. This behavior must be treated as potential evidence of interception or rerouting and investigated accordingly.

📜 Legal Authority and Mandates

T-Mobile, as a federally regulated telecommunications carrier and data handler, is subject to mandatory compliance under the following federal laws and frameworks:

- **Federal Communications Act of 1934**, as amended by the **Telecommunications Act of 1996**, specifically under **Title II** (47 U.S.C. § 201 et seq.) — mandates carriers to provide non-discriminatory service, ensure user privacy, and cooperate in investigations involving unlawful interference or service sabotage.
- **47 U.S. Code § 222** — mandates confidentiality of customer proprietary network information (CPNI), requiring T-Mobile to protect data about location, service usage, and device identifiers from unauthorized access or dissemination.
- **Federal Trade Commission Act (15 U.S. Code § 45)** — prohibits unfair or deceptive trade practices, which include failure to disclose surveillance access, signal tampering, or compromised infrastructure.
- **Computer Fraud and Abuse Act (18 U.S. Code § 1030)** — may apply in instances of unauthorized access to user data or routing manipulation through rogue infrastructure, especially if T-Mobile failed to mitigate or report it.
- **Homeland Security Act of 2002** & **Cybersecurity Information Sharing Act (CISA)** — require telecommunications providers to share verified cybersecurity threats with DHS/CISA and affected individuals.
- **Communications Assistance for Law Enforcement Act (CALEA)** — governs lawful intercepts and mandates full disclosure of any such action; misuse or unauthorized access under this act is a violation.
- **Federal Communications Commission (FCC) Enforcement Mandates** — require prompt reporting of service anomalies, infrastructure vulnerabilities, and suspected signal interception. As a carrier, T-Mobile is also required to file incident reports with:
    - **FCC Enforcement Bureau**
    - **DHS / CISA**
    - **IC3 (Internet Crime Complaint Center)**
    - **U.S. Secret Service Cyber Fraud Task Force (CFTF)** if applicable

  T-Mobile is obligated under these statutes to respond transparently, take corrective action, and protect the civil rights and safety of federally protected individuals—including persons with ADA, Section 504, or VAWA coverage.

- **As a regulated telecommunications carrier, T-Mobile is legally obligated to report network security incidents, privacy breaches, and suspected surveillance or account compromise to the Federal Communications Commission (FCC).** I am formally requesting that T-Mobile fulfill this obligation and file an incident report with the FCC that accurately reflects the concerns I have raised, including but not limited to: unauthorized access, potential interception of calls and data, unexplained tower connections, abnormal routing, service degradation, and my explicit objection to any form of surveillance or metadata harvesting.

  Please confirm in writing that this report has been filed, including the reference number or any case ID issued by the FCC. Failure to comply with federal reporting mandates not only constitutes regulatory negligence but may also amount to obstruction in matters involving protected civil rights and federal investigations.

  You are further requested to immediately file formal reports on my behalf with the appropriate federal authorities, including but not limited to the following:

  - **Internet Crime Complaint Center (IC3)** under the FBI
  - **Cybersecurity and Infrastructure Security Agency (CISA)**
  - **U.S. Secret Service Cyber Fraud Task Force**
  - **U.S. Department of Homeland Security (DHS)**

    These agencies are responsible for investigating and mitigating unauthorized surveillance, telecom-based infrastructure compromise, and cyber-enabled civil rights violations. T-Mobile is in possession of relevant internal metadata, logs, and forensic access records that I, as a civilian, cannot obtain independently. You have an affirmative obligation to disclose and escalate threats to customer safety, especially where known abuse, manipulation of identity infrastructure (SIM, IP, tower routing), or unauthorized third-party access is involved. Please confirm the case numbers, report references, and submission dates for each of these filings.

- **In addition, I am requesting that T-Mobile formally refer this matter to local law enforcement.** I have made multiple attempts to file police reports regarding unlawful interception, infrastructure compromise, and digital targeting, but I have been repeatedly refused by local authorities. T-Mobile, as a carrier with both technical expertise and legal standing, is in a position to escalate this issue appropriately. I am requesting that you file an incident report with the Louisville Metro Police Department or the appropriate jurisdiction and provide me with confirmation that such a report has been made. If jurisdictional confusion exists, you are authorized to contact the Kentucky State Police Cybercrimes Unit or to coordinate with federal law enforcement.

- **I formally demand full disclosure of any instance in which my account, devices, metadata, or communications may have been accessed, reviewed, flagged, shared, or otherwise made available to any third party — including, but not limited to, law enforcement, intelligence agencies, government contractors, external consultants, or undisclosed internal teams.**

  This includes any legal or extralegal requests, backdoor access, shadow reviews, or unlogged administrative interventions, regardless of whether they were initiated via subpoena, national security letter, FISA warrant, informal cooperation, or private agreement.

- **I further request confirmation of whether T-Mobile is currently acting under the direction, influence, advisement, or coercion of any outside entity (governmental, quasi-governmental, or private sector) with regard to my account or communications.** This includes any agency, task force, contractor, or third-party team that may have influenced service decisions, data handling, or administrative behavior toward me or my family.

  Failure to provide a clear and complete response will be interpreted as willful concealment and will be included in evidence related to civil and federal filings already in process.

- Confirm whether my account was ever placed under surveillance, redirection, or internal audit flags
- Reimburse me for **loss of function, hardware replacement costs**, and **damages incurred from digital sabotage**

Failure to respond within **5 business days** will result in the additional filings of **formal complaints with**:

- FCC (Federal Communications Commission)
- FTC (Federal Trade Commission)
- U.S. Secret Service Cyber Fraud Task Force
- Department of Justice Civil Rights Division
- State Attorney General's Office (KY)

IV. Supporting Documentation

Available upon request or by subpoena:

- IC3 Report and CISA Filing
- Packet capture logs, IP route inconsistencies, and Apple diagnostics
- Visual documentation of tower ID spoofing
- Recorded calls and written correspondence showing neglect and evasion by T-Mobile reps

---

V. Customer History and Loyalty

I have been a T-Mobile customer — originally under my mother's account — for over **twenty years**. Despite this long-standing loyalty, I have been treated with **disregard, dismissiveness, and a total lack of due process** in response to urgent, safety-critical issues.

This is not just a customer service failure — it is a breach of **trust** and **duty of care**. After more than two decades with your company, I should not have to fight just to be heard, let alone **prove my existence or the legitimacy of my claims**, while my communications are actively being compromised and my civil rights obstructed.

If T-Mobile has chosen to disregard my safety, loyalty, and federal rights — and that of a disabled child in my care — then you are not simply failing a customer. You are **willfully enabling harm**.

Sincerely,

John R. Fouts, MBA
P. 502.956.0052 (Text Only – ADA Accommodations)

F. 502.996.8246 (HIPAA Compliant)

E. icreateupwardspirals@gmail.com

Whistleblower, Federal ADA Litigant
Louisville, Kentucky
